EXTION

A Project Report On

Investigation of a Data Breach

Submitted in Fulfilment for the Task 2 of

Cyber security Internship

At

Extion Infotech

Submitted by

Hetvi D. Mehta

Table of Contents

Chapter 1 : Objective

This report focuses on the investigation and management of a data breach incident at ABC Secure Bank, a reputable financial institution. The objective is to provide a detailed examination of the incident's origin, progression, and resolution while offering insights into proactive measures for preventing similar incidents in the future. The investigation emphasizes analyzing the breach's technical aspects, its impact on stakeholders, and the necessary compliance and communication strategies.

Key objectives include:

- Identifying the root cause of the breach and potential vulnerabilities.
- Assessing the scope and extent of compromised data.
- Developing effective containment, recovery, and remediation strategies.
- Ensuring compliance with applicable regulations and standards.
- Recommending long-term security improvements for the organization.

Chapter 2 : Scenario Overview

Scenario Description

During a regular security check, ABC Secure Bank, a well-known financial institution, revealed a data breach. Anomalies in database activity logs found during the audit indicated improper access to private client information, such as names, account numbers, and transaction histories. The bank's reputation, regulatory compliance, and consumer privacy were all seriously jeopardized by this hack.

Detailed Scenario

- **Breach Discovery:** Suspicious database access patterns were identified by routine checks.
- **Impact:** Transaction data and personally identifiable information (PII) were made public due to the hack of millions of customer records.
- **Attacker's Methods:** Taking use of a known weakness in an out-of-date software component, particularly an unpatched API endpoint.
- **Exfiltration Timeline:** Because the breach lasted for more than three months, attackers were able to evade detection by exfiltrating data in batches.

Challenges Faced

- **Delayed Detection:** Because of lapses in monitoring, the breach went unnoticed for a long time.
- **Regulatory Pressures:** Compliance with the CCPA and GDPR, as well as timely reporting, were essential.
- **Customer Trust:** Following such an incident, regaining the trust of customers necessitated open communication and aggressive assistance efforts.

Chapter 3 : Tasks and Findings

1. Incident Analysis

1.1 Overview of the Breach

ABC Secure Bank discovered anomalies during a security audit, indicating unauthorized access to sensitive customer data. Immediate concerns included data misuse, legal repercussions, and reputational damage.

1.2 Identification of the Breach

Database logs with odd access patterns were used to identify the incident. Unauthorized access may have continued for months before being discovered, according to analysis, giving attackers plenty of time to take advantage of weaknesses.

1.3 Initial Response

Upon discovery, the bank activated its incident response plan:

- Activated a multidisciplinary incident response team comprising IT security, legal, and communication specialists
- Performed an emergency assessment of critical systems to prioritize containment efforts
- Secured the compromised systems to stop additional harm.

1.4 Point of Entry

According to forensic investigation, hackers took advantage of a flaw in an out-of-date application that was part of the bank's infrastructure. Because patch deployment was delayed, the software component was out of date and susceptible to known attacks.

1.5 Attack Vector

The attackers carried out SQL injection attacks by taking advantage of the unpatched application vulnerability. They got around authentication procedures and gained direct access to private client databases by using fraudulent SQL queries.

Detailed investigation revealed:

- The vulnerability was listed as CVE-XXXX-XXXX in public databases.
- Attackers used automated tools to scan for exploitable endpoints.
- Exploitation occurred through the customer login portal, which lacked input validation and error handling.

1.6 Extent of the Breach

The breach affected critical customer data, including:

- **Names:** Full names of account holders.
- **Account Numbers:** Unique identifiers for individual accounts.
- **Transaction Histories:** Detailed records of recent financial activities.

2. Forensic Analysis

2.1 Evidence Collection

Exact replicas of the compromised systems were made by forensic analysts, who saved logs, configurations, and application states for in-depth analysis. Steps included:

- Imaging hard drives to retain evidence integrity.
- Securing database backups for analysis.
- Using checksum tools to verify evidence authenticity.

2.2 Vulnerability Analysis

A detailed analysis of the out-of-date application was conducted. Among the conclusions were the following:

- The SQL injection vulnerability existed in a deprecated API endpoint.
- Lack of secure coding practices in the application's input handling module.
- Absence of intrusion detection mechanisms at the application layer.

2.3 Log Analysis

Detailed log analysis provided a timeline of events:

- Unpatched endpoints were found via automated scans.
- The hack was preceded by several unsuccessful attempts to log in using dubious IP addresses.
- Within hours after discovery, the SQL injection exploit was successfully exploited.
- To avoid discovery, data was sent in small chunks, according to exfiltration records.

2.4 Timeline

1. **Day 1:** Attackers scanned systems and identified the vulnerable application.
2. **Day 3:** Exploitation began using SQL injection techniques.
3. **Day 7:** Privilege escalation within the database server enabled attackers to extract data.
4. **Month 1 - Month 3:** Exfiltration of customer data occurred intermittently to avoid triggering alarms.
5. **Month 4:** Routine security audit discovered anomalies in database logs, exposing the breach.

3. Data Recovery

3.1 Identifying Exposed Data

Sensitive information exposed during the breach included:

- Customer names and personally identifiable information (PII).
- Detailed account numbers linked to financial assets.
- Historical transaction data spanning several months.

3.2 Recovery Strategy

1. Containment

- Immediate containment measures were implemented to limit the damage and prevent further exploitation:
    - **Isolated Affected Systems:** The vulnerable application was disconnected from the network to halt ongoing data exfiltration.
    - **Applied Patches:** The software was updated to address the SQL injection vulnerability.
    - **Threat Neutralization:** Comprehensive scans were conducted to identify and remove any residual malware.
    - **Enhanced Firewall Rules:** Access to critical systems was restricted based on IP address and access controls.

2. Communication

- Transparent communication was critical to maintaining trust and ensuring stakeholders were informed:
    - **Internal Stakeholders:** Regular updates were provided to executive teams, IT staff, and legal advisors.
    - **Customers:** Personalized notifications detailed the breach and offered clear steps for protecting their information, such as changing passwords and monitoring accounts.
    - **Regulatory Bodies:** Incident reports were submitted to relevant authorities, including timelines, scope, and remediation actions.

3. Customer Support

- To assist affected customers, a dedicated support program was established:
    - **Fraud Monitoring Services:** Free credit monitoring and fraud alert services were offered to all affected customers.
    - **Dedicated Helpdesk:** A 24/7 support helpline was launched to address customer concerns and provide guidance on mitigating risks.
    - **Compensation Measures:** Affected customers were reimbursed for any verified fraudulent activities linked to the breach.

4. Legal and Regulatory Compliance

- Ensuring compliance with local and international data protection regulations was a priority:
    - **GDPR and CCPA Adherence:** Notifications were issued within required timeframes, and data protection impact assessments were conducted.
    - **Legal Coordination:** Legal teams worked closely with law enforcement to identify perpetrators and prepare for potential litigation.
    - **Documentation:** Detailed records of the breach and the recovery process were maintained for audits and compliance reviews.

5. Long-Term Mitigation

- To prevent future breaches, ABC Secure Bank developed and implemented a long-term mitigation plan:
    - **Employee Training:** Regular cybersecurity awareness programs were launched to educate employees on recognizing phishing attempts and social engineering tactics.
    - **Advanced Threat Detection:** Deployment of Security Information and Event Management (SIEM) systems to provide real-time threat intelligence and alerts.
    - **Network Segmentation:** Sensitive systems were isolated within segmented networks to limit access in the event of a breach.
    - **Third-Party Security Audits:** Regular assessments were conducted on third-party vendors to ensure their practices met ABC SecureBank's security standards.
    - **Data Encryption:** All sensitive data was encrypted both at rest and in transit to minimize exposure risks.

4. Regulatory Compliance

Regulatory measures were undertaken to comply with data protection laws:

- **GDPR:** Notified EU-based customers and relevant authorities within the mandated 72-hour window.
- **CCPA:** Provided detailed disclosures to affected California residents.
- **Legal Coordination:** Engaged with legal counsel to assess liabilities and prepare for potential litigation.

5. Communication and Notification

Plan:

1. **Customer Outreach:**
    - Drafted personalized emails to inform customers of the breach.
    - Provided a dedicated support line for inquiries and assistance.
2. **Stakeholder Briefings:**
    - Conducted meetings with board members and key stakeholders to explain the breach's implications and response strategies.
3. **Regulatory Reporting:**
    - Submitted detailed reports to regulatory bodies, including timelines, remediation efforts, and next steps.

6. Post-Incident Review

Security Weaknesses Identified:

- Delays in patch handling have been identified.
- Inadequate secure coding techniques and input validation.
- Inadequate application-layer activity monitoring.

Recommendations:

1. **Automated Patch Management:** To guarantee timely updates for all systems, put in place a centralized patching solution.
2. **Code Reviews and Testing:** To find and fix vulnerabilities, do secure code reviews and penetration tests on a regular basis.
3. **Enhanced Monitoring:** To identify irregularities at the application level, implement real-time monitoring technologies.
4. **Employee Training:** Hold frequent security awareness meetings with an emphasis on threat identification and secure coding.

Chapter 4 : Conclusion

The ABC Secure Bank data breach highlights the complexity of contemporary cyberthreats as well as the dangers associated with antiquated systems, inadequate monitoring, and postponed patching. Vulnerabilities were found, the attack was tracked down, and quick recovery procedures were put in place. Prioritizing regular upgrades, implementing cutting-edge monitoring technologies, improving cybersecurity training for staff members, and keeping a strong incident response strategy are some important lessons learned. ABC Secure Bank can rebuild client confidence and fortify its defences against potential threats by cultivating a culture of ongoing improvement and making smart investments in cybersecurity.